# Exhibit F

AWS Cloud Security  ⌄

Overview

Security Services

Compliance Offerings

Data Protection  ▾

Learning  ▾

Resources  ▾

Partners  ▾
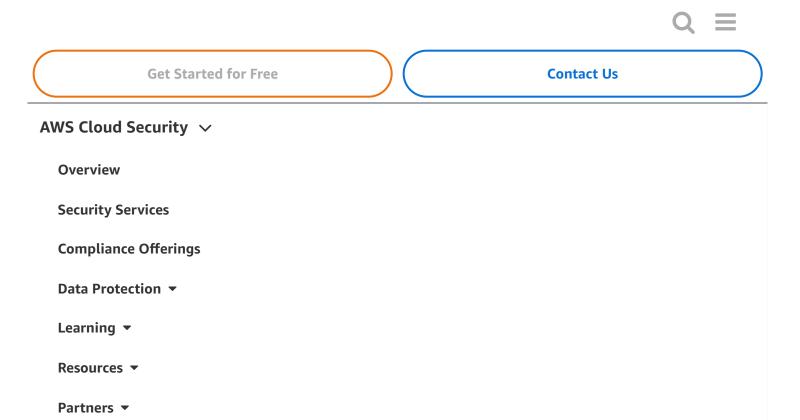
# Data Privacy FAQ

At AWS, customer trust is our top priority. AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to meet their compliance needs. Maintaining customer trust is an ongoing commitment. We strive to inform you of the privacy and data security policies, practices, and technologies we've put in place. Our commitments include:

- **Access:** As a customer, you maintain full control of your content that you upload to the AWS services under your AWS account, and responsibility for configuring access to AWS services and resources. We provide an

advanced set of access, encryption, and logging features to help you do this effectively (e.g., **AWS Identity and Access Management**, **AWS Organizations** and **AWS CloudTrail**). We provide APIs for you to configure access control permissions for any of the services you develop or deploy in an AWS environment. We do not access or use your content for any purpose without your agreement. We never use your content or derive information from it for marketing or advertising purposes.

- **Storage:** You choose the AWS Region(s) in which your content is stored. You can replicate and back up your content in more than one AWS Region. We will not move or replicate your content outside of your chosen AWS Region(s) except as agreed with you.

- **Security:** You choose how your content is secured. We offer you industry-leading encryption features to protect your content in transit and at rest, and we provide you with the option to manage your own encryption keys. These data protection features include:

  - **Data encryption capabilities available in over 100 AWS services**.

  - **Flexible key management options using AWS Key Management Service (KMS)**, allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys.

- **Disclosure of customer content:** We will not disclose customer content (see *How does AWS classify customer information?* below) unless we're required to do so to comply with the law or a binding order of a government body. If a governmental body sends AWS a demand for your customer content, we will attempt to redirect the governmental body to request that data directly from you. If compelled to disclose your customer content to a government body, we will give you reasonable notice of the demand to allow the customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.

- **Security Assurance:** We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our security control environment. These security protections and control processes are independently validated by **multiple third-party independent assessments**.

## What is customer content? ⊕

## What is account information? ⊕

## Who owns customer content? ⊕

Who controls customer content?                                                              ⊕

How do you use my account information?                                                      ⊕

What happens when AWS receives a legal request for customer
content?                                                                                    ⊕

Where is customer content stored?                                                           ⊕

What is my role in securing my content?                                                     ⊕

What steps does AWS take to protect my privacy?                                             ⊕

Who should I contact if I have questions regarding AWS and data
protection?                                                                                 ⊕

How does AWS use information included in resource identifiers
and other items related to the management of AWS resources?                                 ⊕

## Data Privacy Resources

Data Privacy Center

Privacy Features of AWS Services

Amazon Information Requests

AWS Privacy Notice

Using AWS in the Context of Common Privacy &
Data Protection Considerations

Have Questions? Connect with an AWS Business Representative

**Contact Us**

Exploring compliance roles?

**Apply today »**

Want AWS Compliance updates?

**Follow us on Twitter »**

<div>

**Sign In to the Console**

## Learn About AWS

What Is AWS?

What Is Cloud Computing?

AWS Diversity, Equity & Inclusion

What Is DevOps?

What Is a Container?

What Is a Data Lake?

AWS Cloud Security

What's New

Blogs

Press Releases

</div>

## Resources for AWS

Getting Started

Training and Certification

AWS Solutions Library

Architecture Center

Product and Technical FAQs

Analyst Reports

AWS Partners

## Developers on AWS

Developer Center

SDKs & Tools

.NET on AWS

Python on AWS

Java on AWS

PHP on AWS

JavaScript on AWS

## Help

Contact Us

File a Support Ticket

Knowledge Center

AWS re:Post

AWS Support Overview

Legal

AWS Careers

**Create an AWS Account**

Amazon is an Equal Opportunity Employer: *Minority / Women / Disability / Veteran / Gender Identity / Sexual Orientation / Age.*

**Language**

عربي |

Bahasa Indonesia |

Deutsch |

English |

Español |

Français |

Italiano |

Português |

Tiếng Việt |

Türkçe |

Русский |

ไทย |

日本語 |

한국어 |

中文 (简体) |

中文 (繁體)

Privacy

|

Site Terms

|

Cookie Preferences

|

© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.